RECEIVED
CENTRAL FAX CENTER
MAR 07 2008

AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

SUMMARY OF THE INVENTION

[0021] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, an apparatus is provided for performing cryptographic operations. The apparatus includes fetch logic, translation logic, keygen logic, and execution logic. The fetch logic receives a cryptographic instructionsingle atomic cryptographic instruction as part of an instruction flow executing on the microprocessor. The cryptographic ~~instruction~~single atomic cryptographic instruction prescribes one of the cryptographic operations, and also prescribes that a provided cryptographic key be expanded into a corresponding key schedule for employment during execution of the one of the cryptographic operations. The translation logic is coupled to the fetch logic, and is configured to translate thesingle atomic cryptographic instruction into a sequence of micro instructions that directs the microprocessor to perform the one of the cryptographic operations. The keygen logic is disposed within the microprocessor and is operatively coupled to the ~~cryptographic instruction~~single atomic cryptographic instruction. The keygen logic directs the microprocessor to expand the provided cryptographic key into the corresponding key schedule. The execution logic disposed within the microprocessor and is coupled to the keygen logic. The execution logic expands the provided cryptographic key into the corresponding key schedule. The execution logic includes a cryptography unit that executes a plurality of cryptographic rounds on each of the plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, where the plurality of cryptographic rounds are prescribed by a control word that is provided to the cryptography unit.

[0022] One aspect of the present invention contemplates an apparatus for performing cryptographic operations. The apparatus has a cryptography unit disposed within

execution logic in ~~within~~ a microprocessor and keygen logic. The cryptography unit executes one of the cryptographic operations responsive to receipt of a cryptographic ~~instruction~~single atomic cryptographic instruction by the microprocessor within an instruction flow that prescribes the one of the cryptographic operations, where the cryptographic instructionsingle atomic cryptographic instruction is fetched from memory by fetch logic in the microprocessor, and where the ~~cryptographic instruction~~single atomic cryptographic instruction also prescribes that a cryptographic key be expanded into a corresponding key schedule be employed when executing the one of the cryptographic operations. Translation logic in the microprocessor translates the single atomic cryptographic instruction into a sequence of micro instructions that directs the microprocessor to perform the one of the cryptographic operations. The keygen logic is operatively coupled to the cryptography unit. The keygen logic directs the microprocessor to perform the one of the cryptographic operations and to expand the cryptographic key into the corresponding key schedule.

[0023] Another aspect of the present invention provides a method for performing cryptographic operations. The method includes, within a microprocessor, fetching a cryptographic instructionsingle atomic cryptographic instruction from memory that prescribes expansion of a cryptographic key into a corresponding key schedule for employment during execution of one of a plurality of cryptographic operations, and translating the single atomic cryptographic instruction into a sequence of micro instructions that direct the microprocessor to perform the one of the plurality of cryptographic operations; and via a cryptography unit disposed within execution logic in ~~within~~ the microprocessor, ~~executing the cryptographic instruction and~~ expanding the cryptographic key into the corresponding key schedule.

Kindly replace paragraph [0012] with the following amended paragraph:

[0012] To perform cryptographic operations on multiple successive blocks of text, all of the symmetric key algorithms employ the same types of modes. These modes include electronic code book (ECB) mode, cipher block chaining (CBC) mode, cipher feedback (CFB) mode, and output feedback (OFB) mode. Some of these modes utilize an

additional initialization vector during performance of the sub-operations and some use the ciphertext output of a first set of cryptographic rounds performed on a first block of plaintext as an additional input to a second set of cryptographic rounds performed on a second block of plaintext. It is beyond the scope of the present application to provide an in depth discussion of each of the cryptographic algorithms and sub-operations employed by present day symmetric key cryptographic algorithms. For specific implementation standards, the reader is directed to Federal Information Processing Standards Publication 46-3 (FIPS-46-3), dated October 25, 1999 for a detailed discussion of DES and Triple DES, and Federal Information Processing Standards Publication 197 (FIPS-197), dated November 26, 2001 for a detailed discussion of AES. Both of the aforementioned standards are issued and maintained by the National Institute of Standards and Technology (NIST) and are herein incorporated by reference for all intents and purposes. In addition to the aforementioned standards, tutorials, white papers, toolkits, and resource articles can be obtained from NIST's Computer Security Resource Center (CSRC) over the Internet ~~at http://csrc.nist.gov~~.